Financial security management under the conditions of digitalization: the state and business entities

Lesya Yastrubetska[1], Mariia Orel[2], Havrylenko Nataliia[3], Oleksii Tonkykh[4] and Vladymyr Yefimov[5]
Lesya.yastrubetska@lnu.edu.ua, orelmarimail@gmail.com, science-ua@ukr.net, 1402at@gmail.com, efimov2009@i.ua
[1]Department of Finance, Money Circulation and Credit of the Ivan Franko National University of Lviv, Lviv, Ukraine
[2]Department of Public Administration, Interregional Academy of Personnel Management, Kyiv, Ukraine
[3]Faculty of Economics and Business, Department of economics and services, Kyiv National University of Technologies and Design (KNUTD), Kyiv, Ukraine
[4]Faculty of hotel and restaurant and tourist business, Department of hotel and restaurant and tourist business, Kyiv National University of Culture and Arts, Kyiv, Ukraine
[5]Faculty of Training Specialists for Strategic Investigation Units, Department of Financial and Strategic Investigations, Dnipropetrovsk State University of Internal Affairs, Dnipro, Ukraine

Summary
Under the conditions of digitalization, there is a growing need to form mechanisms to protect financial resources to ensure a high level of financial security of business entities. Network technologies cause the emergence of new business models, fundamentally different from the traditional operating structures in industrial corporations. This article aims to assess the state of financial security of business entities in the conditions of digitalization. Methodology. The research conducted a statistical analysis and built linear dependency models based on Eurostat indicators to assess the level of financial security of EU enterprises and the relationship between the indicators of financial security and digitalization. The results show a direct correlation between the share of turnover of enterprises from e-commerce sales and ICT security measures supplied by third parties on behalf of enterprises. Within EU-27 an increase in e-commerce sales is found to encourage companies to implement measures to protect financial resources. A non-linear correlation was found: the growth of turnover from e-sales of companies determines the variation of ICT security measures. Companies within the EU use different protection measures to protect financial resources and implement ICT in-house or by outsourcing. Large and medium-sized companies face more challenges related to ICT and security. Overall, 92% of companies use some form of ICT security measure. Only 24% of EU-27 companies have defined or revised security policies in the past 12 months, while 33% have developed and documented ICT security activities, practices and procedures. In 86% of cases, ICT security measures are implemented either by staff or by outside organizations.

Key words:
capital protection, digitalization, financial security, financial interests, financial risks of enterprises

1. Introduction

Under the conditions of digitalization, there is a growing need for the formation of mechanisms to protect financial resources to ensure a high level of financial security of business entities. Technology, on the one hand, contributes to the optimization of entrepreneurial activity and business processes, information protection, innovation, but, on the other hand, there are new risks associated with the threats of loss of financial resources, illegal transfer of technology, use of intangible assets and intellectual property of entrepreneurs. The networking technology is responsible for the emergence of new business models, fundamentally different from the traditional operating structures in industrial-type corporations. Network communication and e-commerce provide a significant reduction in the transaction costs of enterprises.

Solvency, financial stability, liquidity are indicators of the state of financial security of business entities, on the activities of which depend the economic welfare of the country (job creation, payment of taxes, innovation, and investment). It is entrepreneurs who ensure the production of products, payment of staff, and filling the budget, which requires effective protection of capital, tangible and intangible assets from various kinds of threats. As De Goede [1] notes, “the financial crisis is the biggest threat to national security”, and the economic downturn of 2008-2009, the solvency crisis of 2020-2021, amplified by the impact of the spread of the pandemic, proves the importance of financial security of business entities.

The purpose of the article is to assess the state of financial security of business entities under the conditions of digitalization.

2. Literature review

Over the past twenty years (since the 2000s) there has been a growing concern about corporate financial security [2], [3], [4], [5] and simultaneously the growing popularity of advisory services to investigate financial fraud using technology [6]. Business counseling in the area of

Manuscript received October 5, 2021
Manuscript revised October 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.10.44

financial security involves solving companies' problems related to innovation, education, and risk management [6]. More and more business entities need to protect not just physical assets, but financial, intellectual, information assets. As De Goede [7] notes, the financial security of companies is related to politics, and with the use of technology to establish cross-national communications, technology is an instrument of political influence on companies. Therefore, the financial security of companies is of strategic importance, and effective financial risk management affects the security of the company and determines the ability to exist.

Sosnovska & Zhytar [8] define the concept of financial architecture as a set of interrelated structural elements, such as capital structure, ownership structure and quality of corporate governance, which accumulate and mobilize financial resources, increase control over the activities of the company, eliminate conflicts of interest between owners and other stakeholders. The choice of principles and methods of building financial architecture depends on such financial interests of economic actors as formation of flexible financial potential, optimization of capital structure, increase of investment attractiveness, profit maximization and growth of market value of enterprise. The result of building a flexible financial architecture is to ensure the appropriate level of financial security of the enterprise by identifying, quantifying, neutralizing, minimizing and monitoring its financial risks. Indicators for assessing the level of financial security are classified by its most typical functional components, among which we can distinguish investment, credit, issuance, innovation, and currency. Melnik et al. [9] identify the following fundamental indicators of financial security - financial independence ratio, leverage ratio, accounts receivable turnover ratio, accounts payable turnover ratio, return on assets, return on borrowed capital.

Financial security of the company is considered as an element of economic security, particularly at the national level [10], [11]. Delas, Nosova & Yafinovych [12] highlight the financial interests of business, which are the subject of protection: maximization of owners' welfare, growth of return on capital, sufficiency of financial resources, financial stability, high level of investment activity and return on investment, effective overcoming financial risks, fast overcoming financial crisis.

The study of Belás, Mišanková, Schönfeld & Gavurová [13] reveals a high potential of entrepreneurs for effective financial risk management (especially in company owners with higher education), but at the same time a low level of knowledge in corporate finance management. This leads to the growth of corporate financial risks. That is why it is advisable to develop theoretical and practical knowledge in the field of corporate finance in the context of financial risk management.

Thus, in the scientific literature limited research on the financial security of business entities in the context of digitalization and the introduction of new technologies that transform traditional operating business models.

3. Methodology

The research used Eurostat indicators to assess the level of financial security of EU enterprises and the relationship between the indicators of financial security and digitalization. Statistical analysis and linear dependence models were built to assess:

1. Dependence between the total turnover of e-sales of EU-27 enterprises and ICT security measures.
2. Dependencies between the deviation of total turnover from e-sales of EU-27 enterprises in 2011-2019 and ICT security measures.
3. Dependences of the average growth rate of turnover of EU-27 enterprises (average growth rate 2012-2018) and the share of enterprises with ICT security-related activities carried out by external suppliers or employees.

4. Results

Business digitalization involves the integration of ERP systems for the exchange of information between stakeholders (36% of EU-27 companies implemented such systems in 2019), electronic exchange of invoices for the convenience of automated processing (32% of companies implemented a similar function in 2020), the use of cloud computing technologies (36% of companies use these technologies in their activities within the EU-27 in 2020), integration of big data analysis technologies (13% of companies in the EU-27 countries used big data in their activities as of 2020), integration of 3D technologies printing and robotics (5% of companies in 2020 on average and 17% of large companies), integration of IoT and artificial intelligence technologies (machine learning, speech processing, service work, chatbots - on average, only 2% of EU-27 companies used this technology in 2020 in the EU-27).

Table 1 shows the corporate security policy of companies in the EU-27 countries in 2019, which includes such security measures: strong password authentication, software updates (including operating systems), user identification and authentication using biometric methods implemented by the enterprise, encryption methods data, documents or emails, backing up data to a separate location, network access control, VPN, logging for analysis after security incidents, periodic assessment of the likelihood and impact of ICT incidents, ICT security tests.

Overall, 92% of companies use some form of ICT security measure, but only 24% of EU-27 companies have

defined or revised security policies in the past 12 months, and 33% have developed and documented ICT security activities, practices, and procedures. In 86% of cases, ICT security measures are implemented either by staff or by outside organizations.

Table 1:. Security policy: measures, risks and staff awareness in EU-27 enterprises, % of all enterprises without financial sector, 2019

Percentage of all enterprises without financial sector	2019
ICT security measure used: strong password authentication	76
ICT security measure used: keeping the software (including operating systems) up-to-date	87
ICT security measure used: user identification and authentication via biometric methods implemented by the enterprise	10
ICT security measure used: encryption techniques for data, documents or e-mails	38
ICT security measure used: data backup to a separate location (including backup to the cloud)	76
ICT security measure used: network access control (management of access by devices and users to the enterprise's network)	65
ICT security measure used: VPN (Virtual Private Network extends a private network across a public network to enable secure exchange of data over public network)	42
ICT security measure used: maintaining log files for analysis after security incidents	45
ICT security measure used: ICT risk assessment, i.e., periodically assessment of probability and consequences of ICT security incidents	33
ICT security measure used: ICT security tests	35
Enterprises using any ICT security measure	92
The enterprise's ICT security policy was defined or most recently reviewed within the last 12 months	24
The enterprise's ICT security policy was defined or most recently reviewed more than 12 months and up to 24 months ago	6
The enterprise's ICT security policy was defined or most recently reviewed more than 24 months ago	2
The enterprise's ICT security policy was defined or most recently reviewed within the last 24 months	30
Enterprises have document(s) on measures, practices or procedures on ICT security	33
Enterprises make persons employed aware of their obligations in ICT security related issues by voluntary training or internally available information (e.g., information on the intranet)	42
Enterprises make persons employed aware of their obligations in ICT security related issues by compulsory training courses or viewing compulsory material	22
Enterprises make persons employed aware of their obligations in ICT security related issues by contract (e.g., contract of employment)	36
Enterprises make persons employed aware of their obligations in ICT security related issues	61
Enterprises don't make persons employed aware of their obligations in ICT security related issues	36
The ICT security related activities are carried out by the own employees	40
The ICT security related activities are carried out by external suppliers	65
The ICT security related activities are carried out by own employees or external suppliers	86

Source: Eurostat [14].

Figure 1 shows a direct correlation between the share of enterprise turnover from e-commerce sales and ICT security measures supplied by third parties on behalf of enterprises. The 4% coefficient of determination explains the variation of ICT security measures as a function of enterprise e-commerce sales. It means that an increase in online sales encourages companies to implement financial security measures.

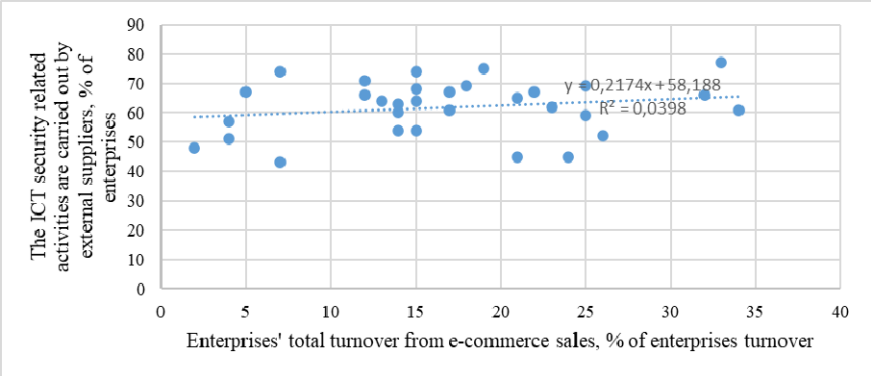

Fig. 1: Dependence between total turnover from e-sales of EU-27 enterprises and ICT security measures (2019)
Source: based on Eurostat [14], [15].

Fig. 2 shows the dependence between the deviation of total turnover from e-sales of EU-27 companies in 2011-2019 (calculated as a standard deviation of turnover) and ICT security measures supplied by third parties or carried out by company employees. The dependence is nonlinear and shows that the growth of turnover from e-sales of companies conditions the variation of ICT security measures.

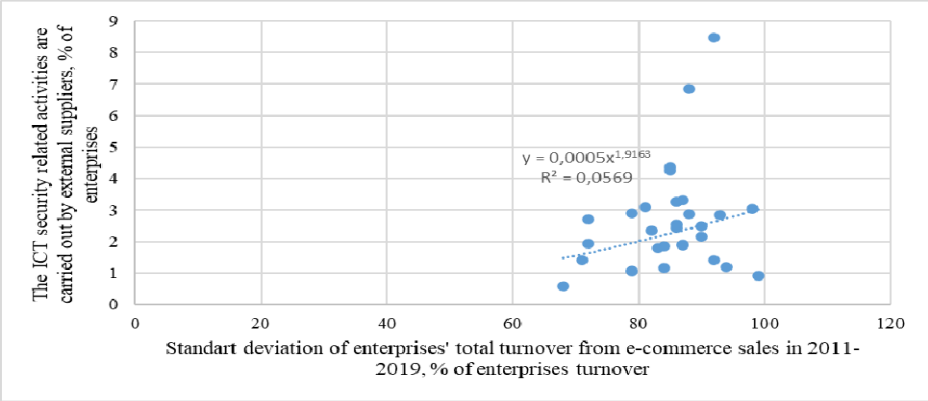

Fig. 2: Dependence between deviation of total turnover from e-sales of EU-27 companies in 2011-2019 and ICT security measures (2019).
Source: based on Eurostat [14], [15].

Thus, companies within the EU use various security measures to protect financial resources and implement ICT in-house or by outsourcing.

Large and medium-sized companies faced more ICT and security challenges (Figure 3). Small businesses were less likely to encounter security problems. The most common problem for businesses was the inaccessibility of ICT services. Although large companies encountered problems with destruction or corruption of data with equal frequency. Disclosure of confidential data is also the most frequent for large companies (4% of recorded cases).

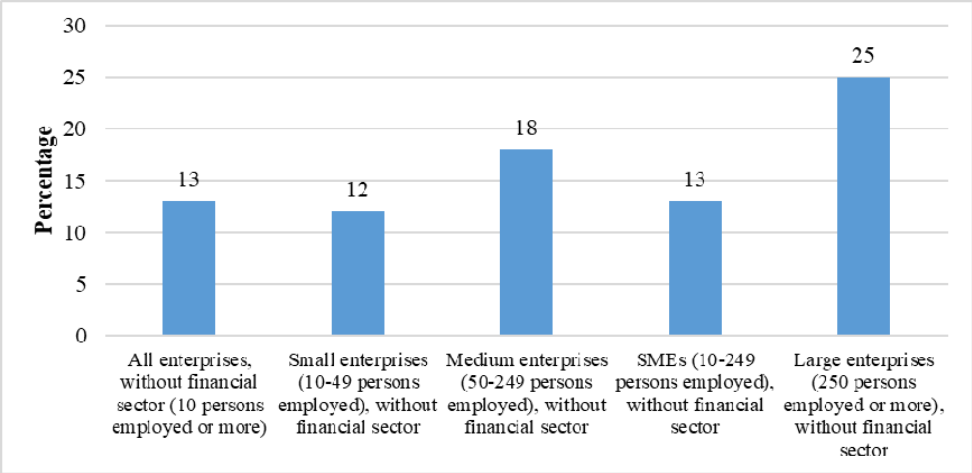

Fig. 3: Enterprises experienced at least once problems due to an ICT related security incident (unavailability of ICT services, destruction or corruption of data, disclosure of confidential data) in EU-27, 2019

Source: based on Eurostat [16].

Figure 4 shows a direct link between the average growth rate of EU-27 companies' turnover and the share of companies implementing security measures with the use of ICT. The linear regression ratio indicates that 1.24% of the variation in security measures is explained by changes in the turnover of goods. The fluctuation of sales volumes determines the safety measures of enterprises.

The turnover of enterprises in various EU countries grew by 2% on average in 2012-2018 (see Fig. 5).

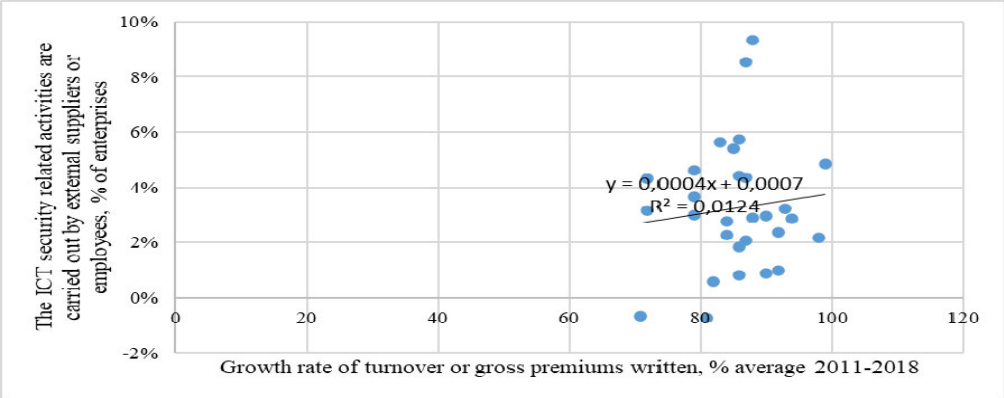

Fig. 4: Relation of the average growth rate of EU-27 enterprises turnover (average growth rate 2012-2018) and share of enterprises with ICT security-related activities performed by external suppliers or employees (2019), % of enterprises

Source: based on Eurostat [16].

The growth rate makes it possible to determine the level of financial risks of enterprises: sharp fluctuations indicate a declining level of financial security, which during a crisis requires a quick response to provide the company with positive cash flow. At the same time, the negative growth rate of turnover was observed in some countries (Greece, Norway, the Czech Republic in 2011-2014, Finland in 2012-2015, Norway and Switzerland). This indicates a decrease in revenues from sales of products, as a result of which the company is exposed to risks of liquidity and payback.

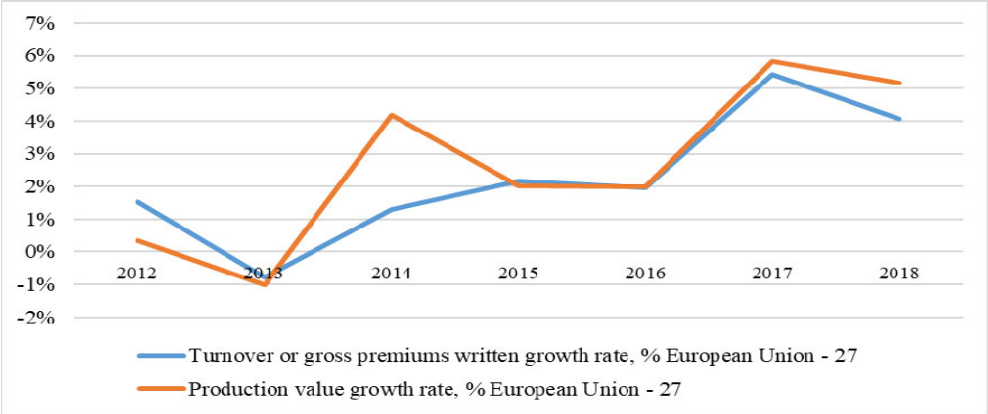

Fig. 5: Growth rate of turnover and volume of enterprises production in the EU-27 in 2012-2018, %
Source: based on Eurostat [17].

Thus, despite certain financial risks and the declining level of financial security of companies in some EU countries, European companies are actively introducing technology and transforming business models and the operational structure of their business activities.

5. Discussion

Several types of research identify the financial security challenges faced by mobile payment services in the Fintech sector in terms of mutual authentication, authorization, integrity, privacy, and accessibility. Since payment services are directly related to users' assets, security is a prerequisite for payment services in the Fintech space [18]. To avoid transferring sensitive user security information to intruders, mobile payment services must be securely constructed from both HW and SW perspectives, and even if multiple payments have been made by the same payment service, payment method information should not be exposed to outsiders without permission [19], [20]. In addition, the information that is used when using the mobile payment service Fintech should not be disclosed [4]. If a secure payment service is not provided, it may not only cause monetary harm to users but also violate user privacy based on the payment information that the user used.

6. Conclusion

The research revealed a direct correlation between the share of enterprises' turnover from e-commerce sales and ICT security measures supplied by third parties by order of enterprises. Within EU-27 the growth of e-commerce sales was found to stimulate companies to implement measures to protect financial resources. A non-linear correlation was found: the growth of turnover from e-sales of companies determines the variation of ICT security measures. Companies within the EU use different protection measures to protect financial resources and implement ICT in-house or by outsourcing. Large and medium-sized companies face more challenges related to ICT and security. Overall, 92% of companies use some form of ICT security measure. Only 24% of EU-27 companies have defined or revised security policies in the past 12 months, while 33% have developed and documented ICT security activities, practices and procedures. In 86% of cases, ICT security measures are implemented either by staff or by outside organizations.

References

[1] M. De Goede, “Financial security,” in The Routledge Handbook of New Security Studies, pp. 112-121, Routledge, 2010
[2] D. Tapscatt, D. Agnew, “Governance in the digital economy,” Finance & Development, 36(004), 2000.
[3] J. W. Williams, “The private eyes of corporate culture: The forensic accounting and corporate investigation industry and the production of corporate financial security,” In Corporate Security in the 21st Century, pp. 56-77. Palgrave Macmillan, London.
[4] J. Kerlin, “The Concept of Resolution of Financial Institutions,” in The Role of Deposit Guarantee Schemes as a Financial Safety Net in the European Union, pp. 137-201, Palgrave Macmillan, Cham, 2017
[5] A. Hopkins, S. Maslen, Risky rewards: How company bonuses affect safety, CRC Press, 2019.
[6] Z. Ćosić, M. Boban, “Business consulting as a point of knowledge of digital economy,” Proc. 33rd International Convention MIPRO, IEEE, pp. 1103-110, 2010, May.
[7] M. De Goede, “Finance/security infrastructures,” Review of international political economy, 28(2), pp. 351-368, 2020.
[8] O.O. Sosnovska, M.O. Zhytar, “Financial architecture as the base of financial safety of the enterprise,” Baltic Journal of Economic Studies, 4(4), pp., 334-340, 2018.
[9] T.E. Melnik, D.E. Lomakin, E.V. Lebedeva, T.G. Aygumov, A.I. Pakhomova, “Applying benchmarking tool in assessment financial safety of organization.” Amazonia Investiga, 9(27), pp. 72-81, 2020.

[10] A. Ahmadi, A. Bouri, "The impact of financial safety act and corporate governance on the level of financial disclosure: case of Tunis stock exchange firms," International Journal of Law and Management, 2016.
[11] G. Blakyta, T. Ganushchak, "Enterprise financial security as a component of the economic security of the state," Investment management and financial innovations, 15(2), pp. 248-256, 2018.
[12] V. Delas, E. Nosova, O. Yafinovych, "Financial security of enterprises," Procedia Economics and Finance, 27, 248-266. 2015. DOI: 10.1016/S2212-5671(15)00998-3
[13] J. Belás, M. Mišanková, J. Schönfeld, B. Gavurová, "Credit risk management: Financial safety and sustainability aspects," Journal of Security and Sustainability Issues, 2017.
[14] Eurostat, "Security policy: measures, risks and staff awareness", https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cisce_ra&lang=en, accessed Aug. 3. 2021.
[15] Eurostat, "Value of e-commerce sales", https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ec_evaln2&lang=en accessed Aug. 3. 2021.
[16] Eurostat, "Security incidents and consequences," https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cisce_ic&lang=en, accessed Aug. 3. 2021.
[17] Eurostat, "Annual enterprise statistics for special aggregates of activities" (NACE Rev. 2). https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do, accessed Aug. 3. 2021.
[18] Y. Yang, Y. Liu, H. Li, B. Yu, "Understanding perceived risks in mobile payment acceptance," Industrial Management & Data Systems, 115(2), pp. 253-269, 2015. DOI: 10.1108/IMDS-08-2014-0243.
[19] J. T. Isaac, Z. Sherali, "Secure mobile payment systems," It professional, 16(3), 36-43, 2014.
[20] T. Zhou, "An empirical examination of initial trust in mobile payment," Wireless personal communications, 77(2), pp. 1519-1531, 2014. C. M. Harris, Handbook of Noise Control, McGraw-Hill, New York, 1978.